

§ 150.313

Federal governmental health plan's or employer's, commitment to the compliance process.

(2) Include the name of the individual in the organization responsible for compliance.

(3) Include an effective monitoring system to identify practices that do not comply with HIPAA requirements and to provide reasonable assurance that fraud, abuse, and systemic errors are detected in a timely manner.

(4) Address procedures to improve internal policies when noncompliant practices are identified.

(g) Evidence documenting the entity's record of previous compliance with HIPAA requirements.

§ 150.313 Market conduct examinations.

(a) *Definition.* A market conduct examination means the examination of health insurance operations of an issuer, or the operation of a non-Federal governmental plan, involving the review of one or more (or a combination) of a responsible entity's business or operational affairs, or both, to verify compliance with HIPAA requirements.

(b) *General.* If, based on the information described in §150.303, CMS finds evidence that a specific entity may be in violation of a HIPAA requirement, CMS may initiate a market conduct examination to determine whether the entity is out of compliance. CMS may conduct the examinations either at the site of the issuer or other responsible entity or a site CMS selects. When CMS selects a site, it may direct the issuer or other responsible entity to forward any documentation CMS considers relevant for purposes of the examination to that site.

(c) *Appointment of examiners.* When CMS identifies an issue that warrants investigation, CMS will appoint one or more examiners to perform the examination and instruct them as to the scope of the examination.

(d) *Appointment of professionals and specialists.* When conducting an examination under this part, CMS may retain attorneys, independent actuaries, independent market conduct examiners, or other professionals and specialists as examiners.

45 CFR Subtitle A (10–1–03 Edition)

(e) *Report of market conduct examination.* (1) *CMS review.* When CMS receives a report, it will review the report, together with the examination work papers and any other relevant information, and prepare a final report. The final examination report will be provided to the issuer or other responsible entity.

(2) *Response from issuer or other responsible entity.* With respect to each examination issue identified in the report, the issuer or other responsible entity may:

(i) Concur with CMS's position(s) as outlined in the report, explaining the plan of correction to be implemented.

(ii) Dispute CMS's position(s), clearly outlining the basis for its dispute and submitting illustrative examples where appropriate.

(3) *CMS's reply to a response from an issuer or other responsible entity.* Upon receipt of a response from the issuer or other responsible entity, CMS will provide a letter containing its reply to each examination issue. CMS's reply will consist of one of the following:

(i) Concurrence with the issuer's or non-Federal governmental plan's position.

(ii) Approval of the issuer's or non-Federal governmental plan's proposed plan of correction.

(iii) Conditional approval of the issuer's or non-Federal governmental plan's proposed plan of correction, which will include any modifications CMS requires.

(iv) Notice to the issuer or non-Federal governmental plan that there exists a potential violation of HIPAA requirements.

§ 150.315 Amount of penalty—General.

A civil money penalty for each violation of 42 U.S.C. 300gg *et seq.* may not exceed \$100 for each day, for each responsible entity, for each individual affected by the violation. Penalties imposed under this part are in addition to any other penalties prescribed or allowed by law.

§ 150.317 Factors CMS uses to determine the amount of penalty.

In determining the amount of any penalty, CMS takes into account the following:

(a) *The entity's previous record of compliance.* This may include any of the following:

(1) Any history of prior violations by the responsible entity, including whether, at any time before determination of the current violation or violations, CMS or any State found the responsible entity liable for civil or administrative sanctions in connection with a violation of HIPAA requirements.

(2) Documentation that the responsible entity has submitted its policy forms to CMS for compliance review.

(3) Evidence that the responsible entity has never had a complaint for non-compliance with HIPAA requirements filed with a State or CMS.

(4) Such other factors as justice may require.

(b) *The gravity of the violation.* This may include any of the following:

(1) The frequency of the violation, taking into consideration whether any violation is an isolated occurrence, represents a pattern, or is widespread.

(2) The level of financial and other impacts on affected individuals.

(3) Other factors as justice may require.

§ 150.319 Determining the amount of the penalty—mitigating circumstances.

For every violation subject to a civil money penalty, if there are substantial or several mitigating circumstances, the aggregate amount of the penalty is set at an amount sufficiently below the maximum permitted by § 150.315 to reflect that fact. As guidelines for taking into account the factors listed in § 150.317, CMS considers the following:

(a) *Record of prior compliance.* It should be considered a mitigating circumstance if the responsible entity has done any of the following:

(1) Before receipt of the notice issued under § 150.307, implemented and followed a compliance plan as described in § 150.311(f).

(2) Had no previous complaints against it for noncompliance.

(b) *Gravity of the violation(s).* It should be considered a mitigating circumstance if the responsible entity has done any of the following:

(1) Made adjustments to its business practices to come into compliance with HIPAA requirements so that the following occur:

(i) All employers, employees, individuals and non-Federal governmental entities are identified that are or were issued any policy, certificate of insurance or plan document, or any form used in connection therewith that failed to comply.

(ii) All employers, employees, individuals, and non-Federal governmental plans are identified that were denied coverage or were denied a right provided under HIPAA requirements.

(iii) Each employer, employee, individual, or non-Federal governmental plan adversely affected by the violation has been, for example, offered coverage or provided a certificate of creditable coverage in a manner that complies with HIPAA requirements that were violated so that, to the extent practicable, that employer, employee, individual, or non-Federal governmental entity is in the same position that he, she, or it would have been in had the violation not occurred.

(iv) The adjustments are completed in a timely manner.

(2) Discovered areas of noncompliance without notice from CMS and voluntarily reported that noncompliance, provided that the responsible entity submits the following:

(i) Documentation verifying that the rights and protections of all individuals adversely affected by the non-compliance have been restored; and

(ii) A plan of correction to prevent future similar violations.

(3) Demonstrated that the violation is an isolated occurrence.

(4) Demonstrated that the financial and other impacts on affected individuals is negligible or nonexistent.

(5) Demonstrated that the non-compliance is correctable and that a high percentage of the violations were corrected.

§ 150.321 Determining the amount of penalty—aggravating circumstances.

For every violation subject to a civil money penalty, if there are substantial or several aggravating circumstances, CMS sets the aggregate amount of the